UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/487,502	01/19/2000	Cynthia Dwork	AM9-99-0138	3238

7590 03/01/2004

John L. Rogitz
Rogitz & Associates
750 B Street, Suite 3120
San Diego, CA 92101

EXAMINER	
SEAL, JAMES	
ART UNIT	PAPER NUMBER
2135	3

DATE MAILED: 03/01/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/487,502	Applicant(s) DWORK ET AL.	
	Examiner James Seal	Art Unit 2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 January 2000*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-35* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-35* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *19 January 2000* is/are: a)□ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. This Action is in response to applicant's application of 19 January 2000.

2. Applicant's IDS has been considered and a signed copy is enclosed with this action. However, the applicant is reminded that non-patent literature as well as patent literature, relavant to the application that is known to the inventors should be filed. This would include, journal articles, proceedings, reports,

3. Claims 1-35 are pending.

Drawings

4. The drawings are objected to because drawings filed with this application are labeled Figure 1 System, Figure 2, Generating Signature at Sender and Figure 5 Verifying Signature at Receiver. Is there also a figure 3 and 4? If not Figure 5 should be relabled 3 and if so they should be included in applicant's response to this action. A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1-11 and 26-35 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The terms "close" in the first claim is relative.

Two points are close in a finite lattice could mean that they are in the same lattice or nearest neighbors.

Claims 12 - 18 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The terms "nearby" in the first claim is relative. Two points are nearby in a finite lattice could mean that they are in the same lattice or nearest neighbors.

Claims 19-25 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The terms " relatively close" in the first claim is relative. Two points are relatively close in a finite lattice could mean that they are in the same lattice or nearest neighbors.

For the purpose of searching for prior are the examiner will take these terms as meaning that the points either fall inside or outside a certain predetermined distance.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ajtai/Dwork A Public-key Cryptosystem with Worst-Case/Average-Case Equivalence, November 8, 1996, and further in view of Diffie/Hellman New Directions in Cryptography

.

6. As per claim 1, the limitation of using a lattice $\mathcal{L}$ (as a computationally hard problem see page 12 section 1) for a public key system is disclosed Ajtai/Dwork see bottom of page 1 and continuing to page 2; page, 4, second complete paragraph from top and pages 13-14. A lattice has a representation in terms of a basis b_1, $b_{2, \ldots} b_n$ for a Lattice $\mathcal{L}$, the basis generates the lattice as follows

$$\mathcal{L}(b_1,\ b_{2, \ldots} b_n) = \{ \sum \lambda_i\, b_i \mid b_1,\ b_{2, \ldots} b_n \in Z \}$$

See page 2 Definitions and in particular page 3 a lattice . The limitation of a random basis for a private key is disclosed page 14, # 1 and the construction of a different random basis for the public key #5. The limitation of using the shortest basis as a point of departure for a hard problem is disclosed page 12 section 1 second paragraph). Thus the private key, which constitutes the computationally hard problem, will be represented by the short basis and the public key will correspond to the dual system. Ajtai/Dwork further disclose encryption and decryption using the lattice on page 14 under that heading. Ajtai/Dwork further disclosed a predetermined distance for the acceptance or rejection of the closeness of two points (see page 4 first complete paragraph from top). Ajtai/Dwork are silent on an associated digital signature which relies on the hard problem of their public key cryptosystem.

Diffie/Hellman disclose the use of public key cryptosystems for digital signing messages that thus authenticating the sender of the message to the recipient (page 35 second column second paragraph from bottom). Diffie/Hellman further teach the use of a one way function f (a hash function) which are easily computable in one direction and computationally *infeasible* to reverse the process as a means of data authentication, to guarantee the authenticity of the message to the receiver (page 35, first column next to last paragraph, page 31, column 2, first compete paragraph). Further these two actions, authenticating the data could be combined into a single action by hashing the message signing the message with the private key of the public key system and then sending the message concatenated with the hashed signature to the recipient. Thus the message would have been referred to the public lattice basis say as a point x and the signature would have been referred to as a point y in the private lattice basis in the lattice $\mathcal{L}$. It would have been obvious to one of ordinary skill in the art at the time of the invention was made to have combined the invention of Ajtai/Dwork with the teachings of Diffie/Hellman (page 35 second column second paragraph from bottom and page 31, column 2, first complete) to have obtain digital signature scheme in a lattice public key system because as Diffie/Hellman point out in section 4, "The problem of authentication is perhaps an even more serious barrier to the universal adoption of telecommunications for business transaction than the problem of key distribution. Authentication is at the heart of any system involving contracts and billing. Without it, business cannot function". Claim 1 is rejected.

7. As per claim 2, the limitation of returning the message point x and the lattice point y as the digital signature is discussed in claim 1. returning both is necessary in order to verify the signature and further determine the authenticity of the message. Claim 2 is rejected.

8. As per claim 3, further comprising randomizing the function f. Diffie/Hellman note (page 36, column 2, second paragraph) that a one way function f is a building function to both encryption functions (e.g. block ciphers) and key generators (pseudorandom sequence). It would have been obvious to one of ordinary skill in the art at the time the invention was made to have continually changed the function f in a random fashion, because all pseudorandom sequences have periods from which the function f can be determined. Randomly changing this function permits the use of this function over a lengthy period of time without compromising the cryptosystem. Claim 3 is rejected.

9. As per claim 4, the limitation that the message f is randomized by concatenating the message μ with a random number ρ. Diffie/Hellman note (last paragraph, column 2) that ciphertext only attacks succeed because the cryptanalysis knows the statistical properties of a language or certain probable words or more generally certain message formats (called cribs) that enable the cryptanalysis to establish certain correspondence between ciphertext and plaintext. The use of *nulls*, as it was known in the nineteenth century or *padding* or *salting* (especially for passwords), adds random text to the message to prevent such attacks from working. It would have been obvious to one of ordinary skill in the art to have padded messages with random text (numbers) to prevent such attacks. Claim 4 is rejected.

10. As per claim 5, the limitation that the function f maps the message μ to a point on a grid disclosed by Diffie/Hellman page 35, column 2 paragraph 2. Diffie/Hellman disclose for the functions suitable for f sparse polynomials over finite field. Thus f maps

μ to a point in the range space of f. Both the domain and range spaces would constitute a finite grid and hence the limitation is met. Claim 5 is rejected.

11. As per claims 6, and 8 the limitation that the function f may be collision intractable is disclosed page 35 second to last paragraph in particular "we are defining a function which is not invertible from a *computational* point of view. Certainly an invertible function is collision intractable and if in addition its inverse is computationally difficult it would serve as a one way function. Further in the same paragraph Diffie/Hellman consider the case of a one way function which has $f(x_1) = y = f(x_2)$ that is they are computationally intensive and have collisions that is for a single y, $x_1 = x_2$. Thus one of ordinary skill in the art at the time the invention was make would have consider forms of f that satisfy both of these conditions in order to increase the security in the case of the collision intractable case or increase flexibility in the case that f allows collisions. Claims 6 and 8 are rejected.

12. As per claim 7, the limitation that the collision intractability of is based on a computational hard problem such as a lattice problem, Diffie/Hellman have pointed out that the one way function f are based on "overwhelmingly" difficult (hard) problems (see column 1 bottom page 35, Diffie/Hellman explain what they mean by overwhelmingly difficult in section 6 in terms of NP complexity) and Ajtai/Dwork teach lattice problems as computationally hard. Thus one of ordinary skill in the art at the time the invention was made would have been motivated to apply the teachings of Diffie/Hellman to the invention disclosed by Ajtai/Dwork because the encryption system already has the lattice problem in place either in software or hardware or both. Claim 7 is rejected.

13. As per claim 9, the limitation that the function f maps the message μ to an auxiliary lattice. Diffie/Hellman disclose that the hard over which the Encryption function (i.e. hard lattice problem disclosed page 14 of Ajtai/Dwork) does not have to be the same in which the function f is based (that is sparse polynomials over a finite field Diffie/Hellman page 35 second comment see Purdy comment), and thus one of ordinary skill in the art at the time the invention was made would have not necessarily been motivated to base both the encryption function and the hashing function on the same hard problem (that is the same lattice or different lattice problems) for security reasons. One might leak more information (bits) in the hashing process than in the encryption process or vice versus and thus might have to use different lattices or even different lattice problems, entirely. Claim 9 is rejected.

14. As per claim 10, the limitation of verifying the digital signature by determining whether the distance between the lattice point x and y vary no more than a predetermine amount. Ajtai/Dwork teach the use of two basis to span a lattice (see page 14, 1-5). Unless these bases are both defined along the same direction and are commeasurable, a point in one representation would not in general be a point in the other basis. Ajtai/Dwork further defined a distance (page 2, lines before the first complete paragraph). That there is a constraint on length for a message or digital signature to be accepted (see second complete paragraph page 4). Claim 10 is rejected.

15. As per claim 11 that the predetermined distance is related to the number of dimensions n in the lattice $\mathcal{L}$. See Ajtai/Dwork top page 4 . Claim 11 is rejected.

16. Claims 12-15 and 17-18 are directed towards a computer program storage device with instructions to implement method claims 1, 6, 3, 4 and 8-9; and are rejected in view of the same prior art of record.

17. As per claim 16, the limitation that f maps the message to a point on a grid was addressed in 5, the limitation of collision intractable was addressed in claim 6 and finally the intractractablity being based on the hardness of the lattice problem was address in claim 7. It would have been obvious for one of ordinary skill in the art at the time the invention was made to have been motivated to combine these features because they each add to the overall security and ease of implementation of the encryption device. Claim 16 is rejected.

18. As per claim 19, a public key encryption/decryption system capable of producing digital signatures for an electronic message, is disclosed by Ajtai/Dwork motified by Diffie/Hellman see discussion in claim 1. Creating a message and representing as a point on the general basis (public key basis) as x and creating a lattice point y on the private key basis which are a predetermined distance apart are disclosed in Ajtai/Dwork see discussion in claim 1. Transmitting the message and x and y and determining the distance between x and y at a remote site fall within the predetermined distance are disclosed in Diffie/Hellman as the function of any public key telecommunication system (see introduction especially first and second paragraph column 1) and Ajtai/Dwork tope page 4. It would have been obvious to one of ordinary skill in the art at the time the invention was made to have combine these separate aspects into a single secure communication system because as Diffie/Hellman discuss in the first paragraph of the

introduction, "we stand today on the brink of revolution in cryptography" which will be able to exploit these aspects in a modern telecommunication environment. Claim 19 is rejected.

19. Claims 20-25 are system limitations incorporated the limitations of claims 16, 4, 6-8, and 11 and are rejected in view of the same prior art of record.

20. As per claim 26, the limitation of generating a lattice $\mathcal{L}$ having at least two basis is disclosed in Ajtai/Dwork page 2 equation at bottom of page and page 14 steps 3-5. Unless the randomly chosen basis is chosen commeasurable with the short basis or parallel the to the short basis it must have a different length and hence there will be a short basis and a long basis. A mapping that maps the concatenation of μ to a point x in an n-demensional space, the message point x being an element of a set of equally spaced points is disclosed Ajtai/Dwork page 2 last equation from bottom. According to the formula, the set to which x belongs to is an n dimensional set of points generating by choosing integers $\lambda_i \in Z$. Thus enumerating all possible integers will generate a set of equally spaced points to which x belongs. The limitation of using the short basis, finding a lattice point y in the lattice $\mathcal{L}$ that is within a predetermined distance of the message point x is disclosed by Ajtai/Dwork see page 1, bottom of page and continuing to top of page 2. Note decryption is determined using a predetermined distance (from a hyperplane) that is the dual to the first basis (or second basis), and again page 4, second complete paragraph from top. Ajtai/Dwork are silent about the use of the public key cryptosystem to develop a digital signature however as discussed in claim 1 and its implementation on a computer base framework, Diffie/Hellman provide the details of

how this can be done see for example page 35 second column third complete paragraph from top. Further Diffie/Hellman disclose the use of public key cryptosystems, in general, to telecommunication and computers see introduction. Claim 26 is rejected.

21. As per claim 27, the limitation that the mapping is undertaken using a function f is met as a mathematical truism. For example see the CRC Concise Encyclopedia of Mathematics by Eric W. Weissten page 1136. "The terms FUNCTION and MAPPING are synonymous with map. Even if this were not considered Ajtai/Dwork as modified by Diffie/Hellman disclose that the mapping process is via a one way function f which in from the standpoint of Diffie/Hellman is necessary in order to determine data intrigrity (page 35 second column), authenticity (page 35 second column) and data security (privacy page 30, bottom and continuing to the second column). Claim 27 is rejected.

22. Claims 28-35, which are dependent on claim 26, parallel claims 4-11, which are dependent on claim 1. Claim 26 recites a method for digitally signing data and does not specify that the long and short basis are associate with the public and private keys whereas claim 1 does. Thus claim 26 broadens the limitations of the invention however addition of the sub limitations would rely on the same prior art and motivation for combining. Claims 28-35 are rejected.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to James Seal whose telephone number is 703 308 4562. The examiner can normally be reached on M-F, 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 703 305 4393. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

James Seal

James Seal
Examiner AU 2135
29 February 2004